Amendments to the Claims

The listing of claims will replace all prior versions, and listings of claims in the application.

1. (Currently Amended) A server to perform computations to establish a secure network session, comprising of:

a system memory; and

a processing unit coupled to said system memory via a system bus, said processing unit obtains values for a modulus N, a private key d, and a cipher text C sent by a client and calculates a value for clear text M for each request for a secure network session made to said server by said client, said processing unit includes:

an execution unit, coupled to a decode unit, configured to execute arithmetic instructions to perform product and square operations, said execution unit including at least two multipliers connected directly with said system memory for multiplying data provided from said system memory, and at least one adder connected directly with said at least two multipliers for applying an addition operation to outputs of said at least two multipliers, said execution unit configurable to perform specified multiplication operations ~~in parallel~~ and ~~configurable to perform~~ specified multiplication and addition operations simultaneously relative to a clock cycle ~~in parallel~~;

said decode unit to receive requests for establishing a secure network session from said client, said decode unit configured to determine if a square operation or a product operation needs to be performed on an operand, said decode unit further configured to issue said arithmetic instructions to said execution unit so that said execution unit performs specified multiplication and addition operations ~~in parallel~~ and

~~performs~~ specified multiplication operations simultaneously relative to the clock cycle ~~in parallel~~ while performing either said square or product operation.

2. - 3. (Cancelled)

4. (Currently Amended) The server of claim [[3]] 1, wherein certain of said multiplication operations are performed ~~in parallel~~ using a multiply and shift by one instruction.

5. - 6. (Cancelled)

7. (Previously Presented) The server of claim 1, wherein said decode unit is further configured to decode an operation $M=C^d \bmod N$ by:

(a) determining a MSB position of an exponent d equal to a first logic state;

(b) issuing a first set of instructions to implement a square and a product operation after said MSB position of said exponent d equal to the first logic state is determined;

(c) determining if a next most significant bit (MSB) of said exponent d is of the first logic state or a second logic state; and either

(d) issuing a second set of instructions to said execution unit to implement a square operation if said next MSB is of said second logic state; or

(e) issuing said first set of instructions to said execution unit if said next MSB said exponent d is of said first logic state to implement a square and a product operation; and

repeating (c) through (e) for every bit in the said exponent d from said next MSB to a least significant bit (LSB).

8. (Previously Presented) The server of claim 7, wherein a final result of said operation $M=C^d \bmod N$ is obtained by accumulating results of (b) through (e).

9. (Previously Presented) The server of claim 1, wherein said encryption processor is located in said server and is used to establish a secure socket layer connection between said server and said client.

10. - 11. (Cancelled)

12. (Previously Presented) The server of claim 1 wherein said product and square operations executed by said execution unit are Montgomery product and square operations.

13. (Cancelled)

14. (Previously Presented) The server of claim 1, wherein said encryption processor is configured into a web server deploying Secure Socket Layer (SSL)/Transport Layer Security(TLS).

15. (Previously Presented) The server of claim 1, wherein said encryption processor is configured into a secure switch deploying Secure Socket Layer (SSL)/Transport Layer Security(TLS).

16. (Previously Presented) The server of claim 1, wherein said encryption processor is configured into an Internet load balance device with Secure Socket Layer (SSL)/Transport Layer Security(TLS) termination functionality.

17. (Previously Presented) The server of claim 1 wherein said encryption processor is configured into an Internet appliance for a Virtual Private Network.

18. (Previously Presented) The server of claim 1 wherein said encryption processor is configured into a security based router.

19. (Previously Presented) The server of claim 1 wherein said encryption processor is configured into a remote access device used for VPN applications.

20. (Previously Presented) The server of claim 1, wherein said encryption processor is configured into one or more of the following: concentrator-based security

systems for enterprise and ISPs; subscriber management systems with VPN support; firewalls with VPN support; and VPN gateways.

21. - 22. (Cancelled)

23. (Currently Amended) The server of claim 1, wherein said at least two multipliers and said at least one adder perform said specified multiplication ~~in parallel~~ in a first clock cycle.

24. (Currently Amended) The server of claim 23, wherein said at least two multipliers and said at least one adder perform said specified multiplication and addition operations ~~in parallel~~ in a second clock cycle that immediately follows said first clock cycle.

25. (Currently Amended) The server of claim 1, wherein said at least two multipliers and said at least one adder perform either specified multiplication operations ~~in parallel~~ or perform specified multiplication and addition operations ~~in parallel~~ in accordance with said arithmetic instructions.

26. (Previously Presented) The server of claim 1, wherein said decode unit determines whether a square operation or a product operation needs to be performed on an operand for a modular operation.

27. (Currently Amended) The server of claim 26, wherein said at least two multipliers and said at least one adder perform either specified multiplication operations ~~in parallel~~ or perform specified multiplication and addition operations ~~in parallel~~ in accordance with the determination of whether a square operation or a product operation needs to be performed.

28. (Previously Presented) The server of claim 1, wherein said arithmetic instructions comprise a set of micro instructions.

29. (Previously Presented) The server of claim 1, wherein said arithmetic instructions comprise plurality of types of add-subtract instructions and a plurality of types of multiply instructions.

30. (Previously Presented) The server of claim 1, wherein said value for clear text M is calculated using said Montgomery method.